**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

| | | |
|---|---|---|
| TIMOTHY NAZZARO, MICHAEL APICELLO, ERIC PIKE, BRIAN MOSEY, DANELLA CLAYTON, and DANIEL MUHLBAUER, on behalf of themselves and all others similarly situated, | ) | |
| Plaintiffs, | ) | |
| v. | ) | 25 C 448 |
| TECTA AMERICA CORP., | ) | |
| Defendant. | ) | |

## MEMORANDUM OPINION

**CHARLES P. KOCORAS, District Judge:**

This putative class action arises out of a data breach incident involving Defendant Tecta America Corp. ("Tecta"), which detected unauthorized access to its information systems in October 2024. Plaintiffs are current and former Tecta employees, and they assert claims of negligence and other state-law causes of action based on the exposure of their personal information in the data breach. Before the Court is Tecta's Motion to Dismiss Plaintiffs' First Amended Class Action Complaint under Federal Rule of Civil Procedure 12(b)(6). For the reasons that follow, the motion is granted in part and denied in part.

## BACKGROUND

The following facts come from the amended complaint and are presumed true

for purposes of this motion. All reasonable inferences are drawn in Plaintiffs' favor.

Tecta is one of the nation's leading commercial roofing companies and is based in Rosemont, Illinois. As a condition of employment, it requires its employees to provide private information, including Social Security numbers, driver's license numbers, and financial account information.

On or around October 1, 2024, Tecta became aware of suspicious activity on some of its computer systems. In response, Tecta began an internal investigation and determined that an unauthorized third party was able to access certain company files between September 20, 2024, and October 2, 2024 (the "Data Breach"). On January 2, 2025, Tecta filed official notice of a hacking incident with the Office of the Attorney General of California. On or around the same time, Tecta also sent out data breach notice letters ("Notices") to individuals whose information was compromised as a result of the Data Breach. Plaintiffs, Timothy Nazzaro, Michael Apicello, Eric Pike, Brian Mosey, Danella Claytor and Daniel Muhlbauer (collectively, "Plaintiffs"), allege that they are current or former employees of Tecta, who each purportedly received a Notice related to the Data Breach.

Nazzaro alleges he has suffered anxiety as a result of the release of his private individuals and has spent several hours of his valuable time dealing with the Data Breach. Apicello alleges he has been subjected to five unauthorized credit pulls resulting in a decrease in credit score and denial of a loan, and has suffered severe emotional distress and anxiety knowing that his name and Social Security number have

been impacted. Pike alleges he suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of his privacy. Mosey has experienced fraudulent charges to his bank account and suspicious spam emails, as well as fear, anxiety, and stress about his private information now being in the hands of cybercriminals. Muhlbauer has suffered anxiety as a result of the release of his private information. Plaintiffs together allege they anticipate spending considerable time and money on an ongoing basis to try and mitigate and address the many harms caused by the Data Breach.

Plaintiffs seek to represent nationwide class of "All individuals in the United States who were impacted by the Data Breach, including all who were sent a notice of the Data Breach." Dkt. # 7, ¶ 175. In their five-count first amended class action complaint ("amended complaint"), Plaintiffs bring claims against Tecta for negligence (Count I), invasion of privacy (Count II), breach of implied contract (Count III), and unjust enrichment (Count IV, pleaded in the alternative to Count III). They also seek a declaratory judgment (Count V) that (1) Tecta owes a legal duty to secure its current and former employees' private information from unauthorized disclosure and theft; (2) Tecta's existing security measures do not comply with its implicit contractual obligations and duties of care with respect to current and former employees' private information; and (3) Tecta continues to breach its legal duty by failing to employ reasonable measures to secure current and former employees' private information. Plaintiffs further seek corresponding prospective injunctive relief requiring Tecta to

employ adequate security protocols consistent with legal and industry standards.

Tecta moves to dismiss the amended complaint in its entirety under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.

## LEGAL STANDARD

A motion to dismiss pursuant to Rule 12(b)(6) for failure to state a claim tests the sufficiency of the complaint, not its merits. *Skinner v. Switzer*, 562 U.S. 521, 529 (2011). To survive a Rule 12(b)(6) motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This pleading standard does not necessarily require a complaint to contain detailed factual allegations. *Twombly*, 550 U.S. at 555. Rather, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014) (quoting *Iqbal*, 556 U.S. at 678).

## DISCUSSION

In its motion, Tecta argues all of Plaintiffs' claims are deficient as a matter of law and must be dismissed. More specifically, Tecta argues: (1) the negligence claim fails because Plaintiffs have not pleaded the requisite elements of duty and damages, and because the claim is by the economic loss doctrine; (2) the invasion of privacy claim fails because Plaintiffs do not allege any intentional intrusion or disclosure by Tecta;

(3) the breach of implied contract claim fails because Plaintiffs failed to allege the existence of any contract sufficient to support such a claim; (4) the unjust enrichment claim fails because Plaintiffs were compensated for their work; and (5) the declaratory judgment claim fails because it is not an independent cause of action. We address each claim and argument in turn.

## I. Count I: Negligence

### A. Choice of Law

As a threshold matter, although Tecta is based in Illinois, none of the Plaintiffs are Illinois residents. Plaintiffs Nazzaro and Muhlbauer are citizens of Kansas, Plaintiffs Apicello and Pike are citizens of Ohio, Plaintiff Mosey is a resident of Florida, and Plaintiff Claytor is a citizen of Texas. Tecta contends that the laws of Plaintiffs' respective home states (Kansas, Ohio, Florida, and Texas)[1] should apply to their negligence claims.

Illinois uses the "most significant relationship" approach of the Restatement (Second) of Conflicts of Law. *Esser v. McIntyre*, 169 Ill. 2d 292 (1996). In applying this test, courts weigh four factors: "(1) where the injury occurred; (2) where the injury-causing conduct occurred; (3) the domicile of the parties; and (4) where the relationship of the parties is centered." *Id.* Generally, the law of the place of injury controls unless

[1] Plaintiffs assert that Tecta hasn't shown how any of the individual state laws will make a difference in the outcome of this case, but simply state that "[a]ll of the state laws apply fundamentally the same standards, and under those standards, Plaintiffs' allegations are sufficient to state their claims against Defendant." Dkt. # 21, at 4. The parties do appear to agree, however, that Illinois law governs Plaintiffs' other claims.

some other jurisdiction has a more significant relationship with the occurrence and with the parties. *Id.*

In the Court's view, it is premature to decide choice of law issues at this stage. *See Mirfasihi v. Fleet Mortg. Corp.*, 450 F.3d 745, 750 (7th Cir. 2006) ("choice-of-law issues in nationwide class actions are rarely so uncomplicated that one can delineate clear winning and losing arguments at an early stage in the litigation."). For purposes of this motion, the Court finds that Illinois has the most significant relationship to this suit. The place of injury factor doesn't offer much guidance because "data breaches are difficult to 'place' in any physical location." *Tate v. EyeMed Vision Care, LLC*, 2023 WL 6383467, at *6 (S.D. Ohio 2023). As for the residence of the parties, Plaintiffs are scattered across four states and seek to certify a nationwide class, which would presumedly increase that count significantly. Tecta's residence and principal place of business is in Illinois, and the allegedly negligent actions by Tecta resulting in the Data Breach would therefore likely have occurred in Illinois. Further factual development may alter the analysis, but for now the Court will apply Illinois law to the negligence claim.

To state a claim for negligence under Illinois law, a plaintiff must allege facts showing that (1) the defendant owed a duty of care to the plaintiff, (2) that the defendant breached that duty, and (3) that the breach was the proximate cause of the plaintiff's injuries. *Cowper v. Nyberg*, 2015 IL 117811, ¶ 13. Tecta argues that Plaintiffs fail to allege a common law duty and cognizable damages, and that the negligence claim is

barred by the economic loss doctrine.

**B. Duty**

The Illinois Supreme Court has not recognized a common law duty to safeguard personal information. Illinois Appellate Courts have reached conflicting conclusions on the issue. *Compare Cooney v. Chi. Pub. Schs*, 407 Ill. App. 3d 358, 363 (2010) (declining to "recognize a 'new common law duty' to safeguard information."), *with Flores v. AON Corp.*, 2023 IL App (1st) 230140, ¶ 24 (finding the reasoning of *Cooney* no longer applies and the "defendant has a common law duty to protect the personal information of its clients"). In 2018, the Seventh Circuit reiterated that "Illinois has not recognized an independent common law duty to safeguard personal information" and found no reason why "the Illinois Supreme Court would likely disagree with the *Cooney* analysis on this issue of duty under the common law . . . ." *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 817 (7th Cir. 2018) (internal citations omitted).

Even in the face of *Schnuck*, though, district courts within the Seventh Circuit have declined to dismiss negligence claims in data breach cases "based on the non-existence of a data security duty under Illinois law." *See In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 590 (N.D. Ill. 2022); *see also In re Mondelez Data Breach Litig.*, 2024 WL 2817489, at *4 (N.D. Ill. 2024) (concluding, based on *Flores*, "the Court is in no position to conclude that, as a matter of law, defendants had no duty to safeguard plaintiffs' personal information."); *Wittmeyer v. Heartland Alliance for*

*Hum. Needs & Rights*, 2024 WL 182211, at *2 (N.D. Ill. 2024) (given the *Flores* court's explanation that "the reasoning of the *Cooney* court no longer applies," the district court "decline[d] to find, as a matter of law, that [the defendant] owed no duty to the plaintiffs to safeguard their personal information."); *Doe v. Genesis Health Sys.*, 2024 WL 3890164, at *10 (C.D. Ill. 2024); *Smith v. Loyola Univ. Med. Ctr.*, 2024 WL 3338941, at 7 (N.D. Ill. 2024). And yet, at least one other district court has gone the other way and rejected *Flores*. *See Doe v. Genesis Health Sys.*, 2025 WL 1000192, at *4 (C.D. Ill. 2025); *Doe v. Chestnut Health Sys.*, 2025 WL 1616635, at *3 (C.D. Ill. 2025) (the conflicting state appellate court opinions "leave[] the Court bound to follow controlling decisions by the Seventh Circuit and the Illinois Supreme Court, neither of which have yet to recognize a common law duty to safeguard personal information.").

Quite recently, however, the Illinois Appellate Court for the First District reversed the dismissal of a negligence claim in a data breach case with similar allegations, essentially accepting without discussion the existence of a common law duty to safeguard personal information. *See Olson v. Ferrara Candy Co.*, 2025 IL App (1st) 241126, ¶ 53 (quoting *Flores* and finding the economic loss doctrine did not bar the plaintiffs' negligence claim because it was based on the employer defendant's "common law duty to safeguard personal information rather than any express contractual duty."). Given all this, this Court also declines to conclude at this stage of the case, as a matter of law, that Tecta had no duty to safeguard Plaintiffs' personal information.

### C. Damages

Next, Tecta argues that Plaintiffs fail to assert a cognizable injury to support their negligence claim, instead alleging "a hodgepodge of generic, speculative, and hypothetical injuries purportedly arising from" the Data Breach. Dkt. # 15, at 13. Illinois law requires a plaintiff to plead "a legally cognizable present injury or damage to sustain a negligence claim." *Leslie v. Medline Indus., Inc.*, 2021 WL 4477923, at *7 (N.D. Ill. 2021) (citation omitted). Plaintiffs allege they have suffered "actual fraud, loss of time and money to address fraud and imminent identity theft, dissemination of their Private Information on the dark web, and increased spam calls since the Data Breach, all of which has resulted in fear, anxiety and stress about the injuries to come." Dkt. # 21, at 8. These allegations are sufficient at this stage. *See*, *e.g.*, *In re Arthur J. Gallagher*, 631 F. Supp. 3d 573, 587 (allegations of emotional harm such as anxiety and increased concerns for the loss of privacy); *Roper v. Rise Interactive Media & Analytics, LLC* ("*Roper II*"), 2024 WL 1556298, at *2 (N.D. Ill. 2024) (anxiety and concern for loss of privacy because of data breach); *Smith*, 2024 WL 3338941, at *7 (fear, anxiety, and worry about the status of, and the loss of control over, private health information sufficient to state a negligence claim under Illinois law).

### D. Economic Loss Doctrine

Lastly, Tecta argues that even if Plaintiffs established a prima facie case for negligence, the claim is nevertheless barred by the economic loss doctrine. "The *Moorman* doctrine, also known as the economic loss doctrine, states that there can be no

recovery in tort for purely economic losses." *Flores*, 2023 IL App (1st) 230140, ¶ 56 (citing *Moorman Mfg. Co. v. Nat'l Tank Co.*, 91 Ill. 2d 69, 88 (1982)). "Economic loss is defined as 'damages for inadequate value, costs of repair and replacement of the defective product, or consequent loss of profits—without any claim of personal injury or damage to other property.'" *Id.* (citation omitted). There are three exceptions to *Moorman*, although none apply here. Nevertheless, the economic loss doctrine does not bar Plaintiffs' negligence claim. *See Olson*, 2025 IL App (1st) 241126, ¶¶ 48–53 (and discussion therein); *Flores*, 2023 IL App (1st) 230140, ¶ 56; *In re Mondelez*, 2024 WL 2817489, at *5 (declining to apply the *Moorman* doctrine to bar a negligence claim based on a law firm's data breach that disclosed the private information of the client's employees). Tecta's motion to dismiss is denied as to Count I.

## II. Count II: Invasion of Privacy

Plaintiffs' invasion of privacy claim alleges intrusion upon seclusion and public disclosure of private facts.

### A. Intrusion Upon Seclusion

To state a claim for intrusion upon seclusion, Plaintiff must allege "(1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering." *Jacobson v. CBS Broad., Inc.*, 2014 IL App (1st) 132480, ¶ 47. The tort is not based on publication or publicity but "depends upon some type of highly offensive prying into the

physical boundaries or affairs of another person." *Lovgren v. Citizens First Nat'l Bank of Princeton*, 126 Ill. 2d 411, 417 (1989); *Bonilla v. Ancestry.com Operations Inc.*, 574 F. Supp. 3d 582, 596 (N.D. Ill. 2021). The act of prying itself must cause the harm in an intrusion upon seclusion claim, and plaintiffs who allege that the publication of private information caused their harm "plead themselves out of court." *Angelo v. Moriarty*, 2016 WL 640525, at *5 (N.D. Ill. 2016); *see also Thomas v. Peral*, 998 F.2d 447, 452 (7th Cir. 1993) ("a plaintiff fails to state a claim for invaded seclusion if the harm flows from publication rather than the intrusion.").

Here, Plaintiffs fail to plead the requisite intentional intrusion. Rather, Plaintiffs argue, without any supporting case law, that they do not need to allege that Tecta "acted with literal intentionality, but merely that Defendant was substantially certain that a failure to implement the safeguards necessary to protect the Private Information would lead to a data breach." Dkt. # 21, at 11–12. "Yet even an allegation that [Tecta] knew better than to configure its security the way it did, or intentionally failed to keep Plaintiffs' PII safe, still falls short of a plausible allegation that [Tecta] intentionally intruded upon Plaintiffs' privacy." *In re Moveit Customer Data Sec. Breach Litig.*, 2025 WL 2179475, at *13–14 (D. Mass. 2025) (cleaned up). Even if Plaintiffs are correct that allegations that Tecta was "substantially certain" would suffice for intentionality, the amended complaint lacks allegations supporting such a claim, and nothing in the amended complaint allows the Court to reasonably infer that Tecta's actions were intentional. *See White v. Citywide Title Corp.*, 2018 WL 5013571, at *3 (N.D. Ill. 2018).

Rather, Plaintiffs' intrusion upon seclusion claim sounds in negligence, and negligence isn't enough. *See Roper v. Rise Interactive Media & Analytics, LLC ("Roper I")*, 2023 WL 7410641, at *8 (N.D. Ill. 2023) (the plaintiffs failed to state an intrusion upon seclusion claim because they did not "allege that Defendant intentionally provided their private information to the hackers; indeed, they allege[d] the opposite—Defendant negligently allowed the hackers to access their data. In other words, it was the hackers, not Defendant, who made the unauthorized intrusion."); *Miller v. NextGen Healthcare, Inc.*, 742 F. Supp. 3d 1304, 1316 (N.D. Ga. 2024) ("the Plaintiffs here do not allege that NextGen participated with the third-party hackers to steal the Plaintiffs' private information. Rather, the claim is predicated on the fact that NextGen did not do enough to fend off the third-party hackers. While the failure to put adequate protections in place may be sufficient for other causes of action, it does not state a claim for intrusion upon seclusion."). Plaintiffs' invasion of privacy claim based on intrusion upon seclusion is dismissed without prejudice.

**B. Public Disclosure of Private Facts**

Plaintiffs also purport to bring an invasion of privacy claim based on public disclosure of private facts. To state this claim under Illinois law, "a plaintiff must allege that: '(1) publicity was given to the disclosure of private facts; (2) the facts were private and not public facts; and (3) the matter made public would be highly offensive to a reasonable person.'" *Anderson v. United Airlines, Inc.*, 2023 WL 5721594, at *3 (N.D. Ill. Sept. 5, 2023) (quoting *Johnson v. K Mart Corp.*, 311 Ill. App. 3d 573, 579 (2000)).

Public disclosure means "communicating the matter to the public at large or to so many persons that the matter must be regarded as one of general knowledge." *Doe v. Fertility Ctrs. of Ill.*, 2022 WL 972295, at *6 (N.D. Ill. 2022).

Tecta argues this claim fails because Plaintiffs have not alleged that their personal information was disseminated in a widespread manner. Plaintiffs respond that "an exception exists where the public disclosure requirement may be satisfied by establishing that a defendant disclosed highly offensive private facts to a person or persons with whom a plaintiff has a special relationship." Dkt. # 21, at 13 (citing *Miller v. Motorola, Inc.*, 202 Ill. App. 3d 976, 981 (1st Dist. 1990)). Plaintiffs say that "the disclosure was done to the exact people from whom cybersecurity measures are meant to protect . . . such that those identity thieves and fraudsters are in a special relationship with Plaintiffs and the Class." Dkt. # 21, at 14.

Courts have routinely found these allegations insufficient to qualify as a public disclosure. *See Roper II*, 2024 WL 1556298, at *3 (collecting cases). Plaintiffs do not allege their relationship with the hacker(s) is different from the plaintiffs in *Roper II* and the cases cited therein. "Plaintiffs' relationship is not made 'special' by the mere fact that the bad actors have Plaintiffs' information and can attempt to use it or sell it to others in the future." *Id.* (citing *Fertility Ctrs.*, 2022 WL 972295, at *6). Plaintiffs' invasion of privacy claim based on public disclosure of private facts is dismissed without prejudice.

## III. Count III: Breach of Implied Contract

To sustain a claim for breach of implied contract, a plaintiff must allege that (1) a contract existed, (2) the plaintiff performed his obligations under that contract, (3) the defendant breached the contract, and (4) the plaintiff suffered damages as a result of that breach. *In re Estate of Khan*, 2021 IL App (1st) 200278, ¶ 28. An implied contract can be created as a result of the parties' actions, even if there is no express contract between them. *Trapani Constr. Co. v. The Elliot Grp., Inc.*, 2016 IL App (1st) 143734, ¶ 41. Under Illinois law, a contract in fact can be implied from the facts and circumstances that demonstrate the parties' intent to be bound. *Olson*, 2025 IL App (1st) 241126, ¶ 59. Unlike an express contract, in which the parties arrive at an agreement using words, an agreement in an implied-in-fact contract is created through the actions and conduct of the parties. *Trapani Constr. Co.*, 2016 IL App (1st) 143734, ¶ 41. "Of course, there must also be a 'meeting of the minds or mutual assent as to the terms of the contract.'" *In re Arthur J. Gallagher*, 631 F. Supp. at 590 (quoting *Nw. Mem'l Healthcare v. Anthem Ins. Cos., Inc.*, 2022 WL 1620025, at *2 (N.D. Ill. 2022)).

Tecta relies on *Archey v. Osmose Utilities Services, Inc.*, 2022 WL 3543469, at *1 (N.D. Ill. 2022), where a former employee alleged a breach of contract claim against his former employer after a cyberattack on the company exposed the plaintiff's private information to an unauthorized third party. The plaintiff alleged that by providing his private information to his employer, he entered into an implied-in-fact contract with the employer whereby it was obligated to take reasonable steps to secure and safeguard his

private information and to take reasonable steps following unauthorized disclosures of such information. *Id.* at *3. The court found that the plaintiff's subjective inference that a contract was formed was not sufficient to allege the element of mutual assent because the plaintiff was required to allege that his employer showed an intention to be bound. *Id.* Essentially, the pleadings lacked two crucial allegations: (1) the employer required the plaintiff to provide his personal information and (2) the plaintiff relied on the employer's privacy policy. *Id.* at *2–3.

Here, Plaintiffs allege that Tecta required them to provide their personal information as a condition of employment, but do not allege reliance on a privacy policy, only reliance on their "reasonabl[e] belie[f] and expect[ation] that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards." Dkt. # 7, ¶ 218. In their response to Tecta's motion to dismiss, Plaintiffs make passing reference to the potential existence of a privacy policy, asserting that the question of whether there is a privacy policy that supports the existence of an implied contract is a question of fact that cannot be resolved at this stage. Indeed, the existence of a privacy policy may very well demonstrate Tecta's "commitment to protecting personal information generally, and it is one of the circumstances that might support an inference of 'an implicit promise to protect employees' personal information in exchange for their employment.'" *In re Mondelez*, 2024 WL 2817489, at *7 (quoting *In re Arthur J. Gallagher*, 631 F. Supp. 3d at 591).

While Tecta stresses that nothing in the amended complaint demonstrates Tecta's agreement to be bound beyond Plaintiffs' own subjective beliefs, "[a]s a matter of common sense, the employer-employee relationship generally encompasses the *implicit* mutual understanding that PII should be kept private and not be subject to public disclosure." *Duffy v. Lewis Bros. Bakeries, Inc.*, 760 F. Supp. 3d 704, 724 (S.D. Ind. 2024) (citing *Johnson v. Nice Pak Prods.*, 736 F. Supp. 3d 639, 651 (S.D. Ind. 2024) ("employees and employers generally understand that PII—necessary for business operations like paying employee wages—should be kept private. Such an understanding is plausibly an implicit term of their employment agreement.")); *see also Olson*, 2025 IL App (1st) 241126, ¶ 60 ("In addition to Ferrara's representations in its privacy policy, it is implied from the relationship between the parties that Ferrara would take reasonable steps to ensure that plaintiffs' personal information would be protected from unauthorized disclosure"); *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *9 (N.D. Cal. 2016) (while the defendant may not have explicitly promised to protect personal information from hackers in the plaintiffs' employment contracts, "it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently"). Plaintiffs' argument on this front is that, given the sensitivity of their information, they "would not have entrusted their Private Information to Tecta in the absence of such an implied contract." Dkt. # 7, ¶ 222. Seems fair enough. The facts and circumstances between

the parties here are sufficient to imply a contract between them for the security of Plaintiffs' personal information. *See Flores*, 2023 IL App (1st) 230140, ¶ 34.

However, Plaintiffs' implied contract claim fails for a very simple reason: to successfully make a breach of implied contract claim under Illinois law, a plaintiff must allege actual monetary damages. *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 149 (2005). The closest Plaintiffs get to this is their allegation that they *may* "incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly related to the Data Breach." Dkt. # 7, ¶ 168. That Plaintiffs "*may* incur" out-of-pocket expenses doesn't cut it. *See*, *e.g.*, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 830 (7th Cir. 2018) ("Money out of pocket is a standard understanding of actual damages in contract law . . ."). And any claims that the time Plaintiffs had to expend to address the consequences of the Data Breach is not sufficient to plausibly show an economic injury for purposes of an implied contract claim. *Flores*, 2023 IL App (1st) 230140, ¶ 35 ("While plaintiffs argue that lost time responding to a data breach meets the standard of actual monetary damages, they rely on federal law rather than Illinois case law."); *id.* at ¶ 43 ("Plaintiffs also cite to *Perdue v. Hy-Vee, Inc.*, [455 F. Supp. 3d 749, 761 (C.D. Ill. 2020)], in which the court held that a plaintiff's time spent monitoring his account due to the data breach was an economic injury; however, this holding was based on federal law and we decline to follow it.").

In the absence of allegations of actual monetary damages, Plaintiffs have failed to plausibly state a breach of implied contract claim under Illinois law. Tecta's motion to dismiss Count III is granted and the claim is dismissed without prejudice.

## IV. Count IV: Unjust Enrichment

In Count IV, Plaintiffs assert a claim for unjust enrichment, pleaded alternatively to the implied contract claim. "To state a cause of action for unjust enrichment, a plaintiff must establish: '(1) the defendant has unjustly retained a benefit to the plaintiff's detriment, and (2) the defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience.'" *MetroPCS v. Devor*, 215 F. Supp. 3d 626, 634–35 (N.D. Ill. 2016) (quoting *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 131 Ill. 2d 145, 137 (1989)). Unjust enrichment is not an independent cause of action. *Gagnon v. Schickel*, 2012 IL App (1st) 120645, ¶ 25. "Rather, it is a condition that may be brought about by unlawful or improper conduct as defined by law, such as fraud, duress or undue influence, and may be redressed by a cause of action based upon that improper conduct." *Charles Hester Enters., Inc. v. Ill. Founders Ins. Co.*, 137 Ill. App. 3d 84, 90–91 (1985), *aff'd*, 114 Ill. 2d 278 (1986).

Here, Plaintiffs allege they conferred a benefit on Tecta by providing Tecta with their private information, which Tecta "profited from . . . and used" for "business purposes." Dkt. #7, ¶¶ 230–31. Plaintiffs have not plausibly alleged Tecta's retention of a benefit conferred by Plaintiffs. "If anything, the consolidated amended complaint suggests that third-party hackers, not Defendants, are the ones who benefitted from the

Data Breach." *In re Arthur J. Gallagher*, 631 F. Supp. 3d at 592; *see also Roper I*, 2023 WL 7410641, at *6 ("Defendant's alleged retention of Plaintiffs' SPI does not confer a benefit on [the defendants] as that term is understood for purposes of unjust enrichment."); *Johnson*, 736 F. Supp. 3d at 652 ("Plaintiffs have not alleged that Defendants benefited from the PII information other than as incidental to benefitting from Plaintiffs' compensated labor. The PII is better understood as necessary to conduct business operations, not a good whose inherent value was extracted by Defendants."). Plaintiff's unjust enrichment claim is dismissed without prejudice.

## V. Count V: Declaratory Judgment

In Count V, Plaintiffs request a declaratory judgment and injunction that addresses Tecta's obligations with respect to safeguarding the personal information it collects. But an injunction and a declaratory judgment are forms of relief; they are not cognizable claims to be pleaded as an independent cause of action. *Sieving v. Cont'l Cas. Co.*, 535 F. Supp. 3d 762, 774 (N.D. Ill. 2021). Thus, the Court grants Tecta's motion to dismiss as to Count V. However, this dismissal does not constitute a decision on the merits as to whether Plaintiffs may be entitled to either form of relief. *See*, *e.g.*, *Garrard v. Rust-Oleum Corp.*, 575 F. Supp. 3d 995, 1004 (N.D. Ill. 2021) (explaining the plaintiff may still seek declaratory relief despite dismissal of his standalone claim for declaratory judgment).

## CONCLUSION

For the foregoing reasons, Tecta's Motion to Dismiss [14] is granted in part and denied in part. Counts II–V are dismissed without prejudice. Plaintiffs may file a second amended complaint by 9/30/2025. A telephonic status hearing is set for 10/7/2025 at 10:10 a.m.

It is so ordered.

Charles P. Kocoras
United States District Judge

Dated: 9/9/2025